REMARKS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-7, 9-15, 17-23, 25-31, 33-39, 41-47 and 49-54 are pending in the present application. Claims 1, 9, 25, 33 and 44 have been amended, and Claims 8, 16, 24, 32, 40 and 48 have been canceled without prejudice.

In the outstanding Office Action, Claims 1-48 were rejected under 35 U.S.C. § 103(a) as unpatentable over of Padgett et al. (U.S. Patent No. 6,535,978, herein "Padgett") in view of Bisbee et al. (U.S. Patent No. 5,615,268, herein "Bisbee").

Claims 1-54 were rejected under 35 U.S.C. § 103(a) as unpatentable over Padgett in view of Bisbee. That rejection is respectfully traversed.

Amended independent Claim 1 is directed to a method for authorizing an electronic data transfer for healthcare transactions that includes receiving an authentication request containing a digital certificate from a requesting device via a communication link, determining whether the digital certificate is valid, creating an authentication response, sending the authentication response to the requesting device via the communication link, and securely storing audit trail information about the electronic data transfer, the digital certificate and at least a portion of the authentication response in a database. Creating the authentication response includes denying the authentication request when the digital certificate is not valid, or approving the authentication request when the digital certificate is valid. Securely storing the audit trail information includes ensuring the long-term data integrity and reliability of the audit trail information such that non-repudiation of the electronic data transfer may be established. The audit trail information about the electronic data transfer includes an electronic document and a date/time stamp of the electronic document.

Amended independent claims 9, 17, 25, 33 and 41 also include authorizing an electronic data transfer for healthcare transactions that includes securely storing audit trail information about the electronic data transfer, the digital certificate and at least a portion of the authentication response. Securely storing the audit trail information includes ensuring the long-term data integrity and reliability of the audit trail information such that non-repudiation of the electronic data transfer may be established. The audit trail information about the

electronic data transfer includes an electronic document and a date/time stamp of the electronic document.

In a non-limiting example, Figures 1, 2 and 5 illustrate a system and method for authorizing (220 and 240) an electronic data transfer for healthcare transactions, such as a transaction relating to a doctor completed screen form 510. The system 100 includes one or more data repositories or vaults (150, 160 or 170) that store the audit trail information necessary to establish non-repudiation for data transfers (see also page 16, lines 17-19). Audit trail information includes individual timestamps for each document (see also page 17, lines 13-15, 17-20). Audit trail information is securely stored 250 such that the long-term data integrity and reliability of the audit trail information is ensured and non-repudiation of the electronic data transfer may be established. Applicants submit that the present invention addresses the verification, validation and non-repudiation requirement of HIPAA (see also page 15, lines 16 and 17). Non-repudiation (*e.g.*, "ensuring the long-term data integrity and reliability of the audit trail information") means that there is a "legal grade" receipt that provides strong and substantial evidence that will make it difficult for the signer to claim that the electronic representation is not valid (see also page 15, lines 17-20). According to the present invention, the presence of an irrefutable date and time stamp, possibly from a third party source, is included in the hashing algorithm – thereby offering complete non-repudiation of origination of the stored and encrypted document. Thereby, the present provides determinable and unalterably conclusive "who" did "what" and "when."

Padgett generally discloses electronic authentication using biological indicia, such as chromosomal DNA, a photograph, scanned fingerprint, iris or retina (see Abstract; col. 2, lines 31-66). A digitized bio-blob is transmitted to a recipient is compared against a bio-blob stored in a bio-blob database that was previously registered by a registrant (see col. 5, line 62 to col. 6, line 42). Padgett does not teach or suggest ensuring the long-term data integrity and reliability of audit trail information such that non-repudiation of the electronic data transfer may be established. Instead, Padgett merely discloses encryption for the purpose of transmitting data from a sender to a recipient. Padgett thus does not teach or suggest ensuring the integrity of data over some period of time or encrypting data after it is transmitted.

Bisbee verifies the integrity of an electronic document based upon "who" generated the electronic document. No mention is made of "when" the electronic document was

created. This is an important component of HIPAA compliance. The timestamp disclosed in Bisbee relates to the when the transmission occurred rather than when the electronic document itself was created. Applicants submit that because Bisbee does not teach or suggest a timestamp associated with "when" the electronic document was created, it cannot be deduced whether an electronic document, though signed by an authorized person was not an original document (*i.e.*, unmodified or recreated – after the fact). With respect to storage of electronic document, Bisbee merely discloses the encryption of the documents themselves by using an asymmetric public / private key encryption scheme. Bisbee fails to teach or suggest a non-repudiable source for "when" an electronic document was created. Applicants submit that Bisbee appears to rely on traditional date methodologies and the integrity / reputation of a trusted third party for origination source dating. Traditional dating methodologies are unreliable in that they are rather susceptible to modification. Trusting independent third parties that use those same methodologies does not ensure "legal grade" non-repudiation.

As stated in M.P.E.P. §2143, a basic requirement for a prima facie case of obviousness is that the prior art reference (or references when combined) must teach or suggest all the claim limitations. As the cited references do not teach or suggest the feature of audit trail information about an electronic data transfer that includes an electronic document and a date/time stamp of the electronic document, it is respectfully submitted the outstanding Office Action has not created a prima facie case of obviousness with regard to the claims dependent from amended independent Claims 1, 9, 17, 25, 33 and 41.

Accordingly, it is respectfully requested this rejection be withdrawn.

CONCLUSION

In light of the arguments set forth above, Applicants respectfully submit that the Application is now in allowable form. Accordingly, Applicants respectfully request consideration and allowance of the currently pending claims.

A three month extension of time fee of $510.00 is due at this time the Commissioner is hereby authorized to deduct this amount as well as any other credits or fees, other than issue fees, that may be required by this paper to Deposit Account No. 07-0153. The Examiner is respectfully requested to call Applicants' Attorney for any reason that would advance the current application to issue. Please reference Attorney Docket No. 124521-1000.

Dated: September 11, 2006.

Respectfully submitted,
GARDERE WYNNE SEWELL LLP

Karl L. Larson
Registration No. 41,141
ATTORNEY FOR APPLICANTS

3000 Thanksgiving Tower
1601 Elm Street
Dallas, Texas 75201-4761
(214) 999-4582 - Telephone
(214) 999-3623– Facsimile

Customer Number 32914